

# VU Research Portal

## Formal Modeling and Analysis of Mobile Ad hoc Networks

Ghassemi Esfahani, F.

2018

### **document version**

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

### **citation for published version (APA)**

Ghassemi Esfahani, F. (2018). *Formal Modeling and Analysis of Mobile Ad hoc Networks*. [PhD-Thesis - Research and graduation internal, Vrije Universiteit Amsterdam].

### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

### **E-mail address:**

[vuresearchportal.ub@vu.nl](mailto:vuresearchportal.ub@vu.nl)

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Problem Statement . . . . .	2
1.2	Analysis Approaches for MANET Protocols . . . . .	3
1.3	Modeling Issues and Challenges . . . . .	4
1.4	Related Work . . . . .	5
1.5	Assumptions, Objective, and Results . . . . .	7
1.6	Organization of Chapters . . . . .	9
1.7	Origins of the Chapters . . . . .	10
<b>2</b>	<b>Preliminaries</b>	<b>11</b>
2.1	Labeled Transition Systems and Semantic Equivalence Relations .	11
2.2	Semantic Model: Constrained Labeled Transition Systems . . . .	12
2.2.1	Unfolding a CLTS into an LTS . . . . .	13
2.3	Computed Network Process Theory . . . . .	15
2.3.1	Data Types . . . . .	15
2.3.2	CNT Syntax and Semantics . . . . .	16
2.3.3	Rooted Branching Computed Network Bisimilarity . . . .	20
2.3.4	Axioms . . . . .	21
2.3.5	Symbolic Verification . . . . .	25
2.4	Actor Model and the Rebeca Language . . . . .	32
<b>3</b>	<b>Reliable Restricted Broadcast Process Theory</b>	<b>37</b>
3.1	Extending Network Constraints . . . . .	39
3.1.1	Reliable versus Unreliable Communication . . . . .	39
3.1.2	Unfolding a CLTS into an LTS . . . . .	40
3.2	Syntax and semantics of <i>RRBPT</i> . . . . .	40
3.2.1	Operational Semantics . . . . .	42
3.3	Rooted Branching Reliable Computed Network Bisimilarity . . . .	44
3.4	Axioms . . . . .	46
3.5	Case Study: a Simple Routing Protocol . . . . .	52
3.5.1	Protocol Specification . . . . .	52
3.5.2	Protocol Analysis . . . . .	55
3.6	Case Study: Leader Election Algorithm . . . . .	58

3.6.1	Protocol Specification . . . . .	58
3.6.2	Tool Support . . . . .	62
3.6.3	Protocol Analysis . . . . .	65
3.7	Related Work . . . . .	65
3.7.1	Modeling Issues . . . . .	66
3.7.2	Analysis Approaches . . . . .	69
3.8	Conclusion . . . . .	70
<b>4</b>	<b>Wireless Rebeca</b> . . . . .	<b>73</b>
4.1	Counter Abstraction . . . . .	75
4.2	Modeling Topology and Mobility . . . . .	76
4.3	wRebeca: Syntax and Semantics . . . . .	77
4.3.1	Syntax . . . . .	77
4.3.2	Semantics . . . . .	79
4.4	Semantic Reduction Techniques . . . . .	85
4.4.1	Applying Counter Abstraction . . . . .	85
4.4.2	Eliminating $\tau$ -Transitions . . . . .	90
4.5	Modeling the AODVv2 Protocol . . . . .	92
4.5.1	Evaluating Route Messages . . . . .	96
4.5.2	Updating the Routing Table . . . . .	96
4.5.3	<i>rreq</i> Message Server . . . . .	97
4.5.4	<i>rrep</i> Message Server . . . . .	100
4.5.5	<i>rerr</i> Message Server . . . . .	102
4.5.6	<i>newpkt</i> Message Server . . . . .	102
4.6	Evaluation . . . . .	102
4.6.1	State Space Generation . . . . .	104
4.6.2	Tool Support . . . . .	107
4.6.3	Model Checking of the AODV Protocol Properties . . . . .	108
4.7	Related Work . . . . .	111
4.8	Conclusion . . . . .	112
<b>5</b>	<b>Model Checking MANETs</b> . . . . .	<b>115</b>
5.1	Restricting Semantics with Network Constraints . . . . .	116
5.2	Constrained Action Computation Tree Logic (CACTL) . . . . .	117
5.2.1	Motivating Example . . . . .	117
5.2.2	CACTL Syntax . . . . .	118
5.2.3	CACTL Semantics . . . . .	121
5.3	Model Checking Algorithms . . . . .	121
5.3.1	Model Checking <b>EU</b> Formulae . . . . .	122
5.3.2	Model Checking <b>AU</b> Formulae . . . . .	124
5.3.3	Model Checking <b>EW</b> Formulae . . . . .	128
5.3.4	Model Checking <b>AW</b> Formulae . . . . .	129
5.4	Protocol Analysis with CACTL . . . . .	129
5.4.1	Checking the Packet Delivery Property of AODV . . . . .	130

5.4.2	Verification of the Leader Election Algorithm . . . . .	131
5.5	Related Work . . . . .	132
5.6	Conclusion . . . . .	133
<b>6</b>	<b>Product Line Process Theory</b>	<b>135</b>
6.1	PL-CCS : Syntax and Semantics . . . . .	139
6.1.1	PL-CCS: Syntax . . . . .	139
6.1.2	PL-CCS Semantics . . . . .	141
6.2	Bisimilarity for Product Line . . . . .	143
6.2.1	Equivalence Relation . . . . .	144
6.2.2	Congruence Property . . . . .	149
6.3	Equational Reasoning on PL-CCS Terms . . . . .	151
6.3.1	Extending PL-CCS Framework . . . . .	152
6.3.2	PL-CCS Axiomatization . . . . .	152
6.3.3	Completeness of the Axiomatization for Finite-state Behav- iors . . . . .	156
6.4	Product Line Analysis . . . . .	156
6.4.1	Deriving Products of a Family . . . . .	157
6.4.2	Restructuring a Product Family . . . . .	158
6.5	Logical Characterization . . . . .	160
6.5.1	Multi-Valued Modal $\mu$ -Calculus . . . . .	161
6.5.2	Relation to Product Line Bisimilarity . . . . .	162
6.6	Related Work . . . . .	162
6.7	Conclusions and Future Work . . . . .	164
<b>7</b>	<b>Concluding Remarks</b>	<b>167</b>
7.1	Results . . . . .	167
7.2	Future Work . . . . .	169
	<b>Bibliography</b>	<b>171</b>
<b>A</b>	<b>Proofs of Chapter 3</b>	<b>185</b>
A.1	Proof of Theorem 3.2 . . . . .	185
A.2	Proof of Theorem 3.5 . . . . .	189
A.3	Soundness of RCNT Axiomatization . . . . .	194
A.4	Completeness of RCNT Axiomatization . . . . .	196
A.5	Proofs of Section 3.5.2 . . . . .	197
A.5.1	Proof of Theorem 3.7 . . . . .	197
A.5.2	Proof of Proposition 3.8 . . . . .	199
<b>B</b>	<b>Proofs of Chapter 6</b>	<b>201</b>
B.1	Proofs of Theorems 6.5, 6.10, and 6.12 . . . . .	201
B.1.1	Proof of Theorem 6.5 . . . . .	201
B.1.2	Proof of Theorem 6.12 . . . . .	201

B.1.3	Proof of Theorem 6.10 . . . . .	206
B.2	Proof of Theorem 6.13 and 6.20 . . . . .	209
B.3	Soundness of Axiomatization . . . . .	211
B.4	Ground-Completeness of Axiomatization . . . . .	213
B.5	Proof of Theorem 6.24 . . . . .	215
<b>Summary</b>		<b>219</b>
<b>Samenvatting</b>		<b>221</b>